日　本　国　特　許　庁
JAPAN　PATENT　OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application:　２００２年　９月２６日

出願番号
Application Number:　特願２００２－２８０２８９

[ST.10/C]:　[ＪＰ２００２－２８０２８９]

出願人
Applicant(s):　株式会社東芝

２００３年　３月　７日

特許庁長官
Commissioner,
Japan Patent Office　太田信一郎

出証番号　出証特２００３－３０１４０９０

【書類名】　特許願
【整理番号】　13B0250501
【あて先】　特許庁長官殿
【国際特許分類】　H04L 12/00
【発明の名称】　サーバ計算機保護装置、サーバ計算機保護方法、サーバ計算機保護プログラム及びサーバ計算機
【請求項の数】　10
【発明者】
【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝　研究開発センター内
【氏名】　菅野　伸一
【発明者】
【住所又は居所】　東京都府中市東芝町１番地　株式会社東芝　府中事業所内
【氏名】　楯岡　正道
【特許出願人】
【識別番号】　000003078
【氏名又は名称】　株式会社　東芝
【代理人】
【識別番号】　100083161
【弁理士】
【氏名又は名称】　外川　英明
【電話番号】　(03)3457-2512
【手数料の表示】
【予納台帳番号】　010261
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

出証特２００３－３０１４０９０

【書類名】　明細書

【発明の名称】　サーバ計算機保護装置、サーバ計算機保護方法、サーバ計算機保護プログラム及びサーバ計算機

【特許請求の範囲】

【請求項１】

不特定のクライアント計算機によるDoS攻撃からサーバ計算機を保護するサーバ計算機保護装置において、

クライアント計算機から送られてくるデータ要求をサーバ計算機の代わりに受け付けるデータ要求受け付け手段と、

一定期間内に、すべてのクライアント計算機から届いたデータ要求の数を計測するデータ要求数計測手段と、

一定期間内に前記サーバ計算機から前記クライアント計算機へ応答した数を計測するデータ応答数計測手段と、

前記データ応答数計測手段及びデータ要求数計測手段の出力結果を用いて前記サーバ計算機の負荷状態を求めるサーバ負荷算出手段と、

前記サーバ負荷算出手段によって求めた負荷状態に応じて、一定期間内に前記データ要求受け付け手段が受け付けたデータ要求のうちの、該受け付けたデータ要求数に対する一定期間内に前記サーバ計算機へ転送するデータ要求の数の割合を変化させるデータ要求転送手段と、

を備えたことを特徴とするサーバ計算機保護装置。

【請求項２】

不特定のクライアント計算機によるDoS攻撃からサーバ計算機を保護するサーバ計算機保護装置において、

所定のクライアント計算機から送られてくるデータ要求をサーバ計算機の代わりに受け付けるデータ要求受け付け手段と、

一定期間内に、前記所定のクライアント計算機から届いたデータ要求の数を計測するデータ要求数計測手段と、

一定期間内に前記サーバ計算機が前記所定のクライアント計算機へ応答した数を計測するデータ応答数計測手段と、

前記データ要求数計測手段及びデータ応答数計測手段の出力結果を用いて、前記所定のクライアント計算機に対するサーバ計算機の負荷状態を求めるサーバ負荷算出手段と、

前記サーバ負荷算出手段によって求めた負荷状態に応じて、一定期間内に前記データ受け付け手段が受け付けた前記所定のクライアント計算機から送られてくるデータ要求のうちの、該受け付けたデータ要求数に対する一定期間内に前記サーバ計算機へ転送するデータ要求の数の割合を変化させるデータ要求転送手段と、

を備えたことを特徴とするサーバ計算機保護装置。

【請求項３】

前記データ要求転送手段は、前記サーバ負荷算出手段が求めた前記サーバ計算機の負荷状態から、以前よりも負荷が高くなったと判断した場合は前記サーバ計算機へ転送するデータ要求の数の割合をより低く設定し、

一方、以前よりも負荷が低くなったと判断した場合は前記サーバ計算機へ転送するデータ要求の数の割合をより高く設定することを特徴とする請求項１または請求項２に記載のサーバ計算機保護装置。

【請求項４】

不特定のクライアント計算機によるDoS攻撃からサーバ計算機を保護するサーバ計算機保護方法であって、

クライアント計算機から送られてくるデータ要求をサーバ計算機の代わりに受け付けるステップと、

一定期間内に、すべてのクライアント計算機から届いたデータ要求の数を計測するステップと、

一定期間内に前記サーバ計算機から前記クライアント計算機へ応答した数を計測するステップと、

前記データ要求数及び応答数を用いて前記サーバ計算機の負荷状態を求めるステップと、

前記求めた負荷状態に応じて、一定期間内に受け付けた前記データ要求のうちの、該受け付けたデータ要求数に対する一定期間内に前記サーバ計算機へ転送す

るデータ要求の数の割合を変化させるデータ要求転送ステップと、
を有することを特徴とするサーバ計算機保護方法。

【請求項５】

不特定のクライアント計算機によるDoS攻撃からサーバ計算機を保護するサーバ計算機保護方法であって、

所定のクライアント計算機から送られてくるデータ要求をサーバ計算機の代わりに受け付けるステップと、

一定期間内に、前記所定のクライアント計算機から届いたデータ要求の数を計測するステップと、

一定期間内に前記サーバ計算機が前記所定のクライアント計算機へ応答した数を計測するステップと、

前記データ要求数及び応答数を用いて、前記所定のクライアント計算機に対するサーバ計算機の負荷状態を求めるステップと、

前記求めた負荷状態に応じて、一定期間内に受け付けた前記所定のクライアント計算機から送られてくるデータ要求のうちの、該受け付けたデータ要求数に対する一定期間内に前記サーバ計算機へ転送するデータ要求の数の割合を変化させるデータ要求転送ステップと、
を有することを特徴とするサーバ計算機保護方法。

【請求項６】

前記データ要求転送ステップは、求めた前記サーバ計算機の負荷状態から、以前よりも負荷が高くなったと判断した場合は前記サーバ計算機へ転送するデータ要求の数の割合をより低く設定し、

一方、以前よりも負荷が低くなったと判断した場合は前記サーバ計算機へ転送するデータ要求の数の割合をより高く設定することを特徴とする請求項４または請求項５に記載のサーバ計算機保護方法。

【請求項７】

不特定のクライアント計算機によるDoS攻撃からサーバ計算機を保護するサーバ計算機保護プログラムであって、

所定のクライアント計算機から送られてくるデータ要求をサーバ計算機の代わ

りに受け付けるステップと、

一定期間内に、前記所定のクライアント計算機から届いたデータ要求の数を計測するステップと、

一定期間内に前記サーバ計算機が前記所定のクライアント計算機へ応答した数を計測するステップと、

前記データ要求数及び応答数を用いて、前記所定のクライアント計算機に対するサーバ計算機の負荷状態を求めるステップと、

前記求めた負荷状態に応じて、一定期間内に受け付けた前記所定のクライアント計算機から送られてくるデータ要求のうちの、該受け付けたデータ要求数に対する一定期間内に前記サーバ計算機へ転送するデータ要求の数の割合を変化させるデータ要求転送ステップと、

を有することを特徴とするサーバ計算機保護プログラム。

【請求項８】

前記データ要求転送ステップは、求めた前記サーバ計算機の負荷状態から、以前よりも負荷が高くなったと判断した場合は前記サーバ計算機へ転送するデータ要求の数の割合をより低く設定し、

一方、以前よりも負荷が低くなったと判断した場合は前記サーバ計算機へ転送するデータ要求の数の割合をより高く設定することを特徴とする請求項７に記載のサーバ計算機保護プログラム。

【請求項９】

クライアント計算機からの要求に応じたデータを供給するサーバ計算機であって、

所定のデータ要求を処理して、該データ要求をしたクライアント計算機に供給するデータを作成するデータ処理手段と、

所定のクライアント計算機から送られてくるデータ要求を受け付けるデータ要求受け付け手段と、

一定期間内に、前記所定のクライアント計算機から届いたデータ要求の数を計測するデータ要求数計測手段と、

一定期間内に、前記所定のクライアント計算機へ応答した数を計測するデータ

応答数計測手段と、

前記データ要求数計測手段及びデータ応答数計測手段の出力結果を用いて、前記所定のクライアント計算機に対する負荷状態を求めるサーバ負荷算出手段と、

前記サーバ負荷算出手段によって求めた負荷状態に応じて、一定期間に前記データ受け付け手段が受け付けた前記所定のクライアント計算機から送られてくるデータ要求のうちの、該受け付けたデータ要求数に対する一定期間内に前記データ処理手段へ転送するデータ要求の数の割合を変化させるデータ要求転送手段とを備え、

不特定のクライアント計算機からのDoS攻撃を受けたときに、正当なデータ要求を行っていた所定のクライアント計算機からのデータ要求、および正当なデータ要求を行っているにもかかわらず、DoS攻撃を行っていると判断された所定のクライアント計算機からのデータ要求が継続して処理されること特徴とするサーバ計算機。

【請求項１０】

前記データ要求転送手段は、前記サーバ負荷算出手段が求めた前記サーバ計算機の負荷状態から、以前よりも負荷が高くなったと判断した場合は前記サーバ計算機へ転送するデータ要求の数の割合をより低く設定し、

一方、以前よりも負荷が低くなったと判断した場合は前記サーバ計算機へ転送するデータ要求の数の割合をより高く設定することを特徴とするサーバ計算機保護装置を備えた請求項９に記載のサーバ計算機。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】　本発明は、クライアントとなる計算機とサーバとなる計算機間のネットワークシステムに関し、特に、意図的にサーバ計算機の処理を妨害する不正なアクセスからサーバとなる計算機を保護するサーバ計算機保護装置に関する。

【０００２】

【従来の技術】

近年、インターネット等を利用し、不特定あるいは特定のクライアントとなる

計算機をネットワーク経由でサーバとなる計算機に接続し、クライアントからの要求に応じてサーバからデータを供給することを目的とするクライアント・サーバシステムが広く使われている。

【０００３】

インターネット等のネットワークを流れるデータの形式として、宛先情報を付して伝送データを所定の大きさに再構成したパケットが一般に利用されている。パケットは、大まかに分けると、ヘッダとデータ本体とで構成されている。ヘッダには、このパケットの送り元である送信元の計算機を示すＩＰ(Internet Protocol)アドレスと、このパケットの宛先となる計算機のＩＰアドレスといったアドレス情報をもっている。

【０００４】

昨今、このようなネットワークに接続されたシステムに対し、システム的な障害を発生させることを目的としたネットワーク越しの攻撃が増加する傾向にある。たとえば、一つのクライアントから同時に大量のアクセス要求をサーバ計算機に対して行うことにより、攻撃対象となるサーバの稼動を妨げ実質的にサービスを不能にする攻撃方法(以下、DoS攻撃(Denial of Service attack)と表記)がある。

【０００５】

この攻撃方法は、システム攻撃を意図しない正当なクライアントからのアクセスとの区別がつきにくいために、サーバ側で攻撃を回避することが極めて困難である。場合によっては複数のクライアントからこの攻撃を受けることもあり、これを特にDDoS攻撃(Distributed Denial of Service attack)と呼んでいる。

【０００６】

サーバへの要求がサーバの処理能力を超えるほど大量に送りつけられると、その要求毎に通信処理用の資源、たとえばメモリ領域や回線の帯域などが次々と確保されるためついには不足を来たし、妨害を意図していない正当なクライアントからの要求に対しサーバが応答できなくなるか、あるいは大きく滞ってしまうという結果を招く。

【０００７】

従来は、これらの攻撃を排除するためにサーバとネットワークの間にサーバ計算機保護装置を配置していた。このサーバ計算機保護装置は、複数回のアクセス要求が繰り返されたもののみを正当なアクセス要求として処理する、または既に正当なアクセスがあったクライアントからのアクセスを正当なアクセス要求として処理し、それ以外のアクセスについてはパケットを破棄するなどの処理を行っていた。

【０００８】

しかし、このような方法では、攻撃を意図するクライアントが同じような大量のアクセス要求を行う場合、攻撃を排除できないという問題点があった。

【０００９】

一方、上記問題を解決しても、たとえば特定のクライアントが大量のアクセス要求を行うとその通信行為がDoS攻撃であると判断されてしまうため、たとえそれが正当な要求であっても不正なアクセスとみなされる場合があった。DoS攻撃とみなされれば判断されたクライアントの接続は切断されてしまうため、そのクライアントで行っている業務に支障を来たす。

【００１０】

【特許文献１】　特開２００２－１６６３３公報

【００１１】

【発明が解決しようとする課題】

本発明は、不特定のクライアントからのDoS攻撃からサーバとなる計算機を保護しながらも、正当なアクセスを行っているクライアントでありながらDoS攻撃を行っていると判断された計算機のアクセスも限定的に許容するサーバ計算機保護装置、サーバ計算機保護方法、サーバ計算機保護プログラム及びサーバ計算機を提供することを目的とする。

【００１２】

【課題を解決するための手段】

本発明にかかるサーバ計算機保護装置とすれば、

不特定のクライアント計算機によるDoS攻撃からサーバ計算機を保護するサーバ計算機保護装置において、

クライアント計算機から送られてくるデータ要求をサーバ計算機の代わりに受け付けるデータ要求受け付け手段と、

一定期間内に、すべてのクライアント計算機から届いたデータ要求の数を計測するデータ要求数計測手段と、

一定期間内に前記サーバ計算機から前記クライアント計算機へ応答した数を計測するデータ応答数計測手段と、

前記データ応答数計測手段及びデータ要求数計測手段の出力結果を用いて前記サーバ計算機の負荷状態を求めるサーバ負荷算出手段と、

前記サーバ負荷算出手段によって求めた負荷状態に応じて、一定期間内に前記データ要求受け付け手段が受け付けたデータ要求のうちの、該受け付けたデータ要求数に対する一定期間内に前記サーバ計算機へ転送するデータ要求の数の割合を変化させるデータ要求転送手段と、

を備えたことを特徴とするサーバ計算機保護装置

が提供される。

【００１３】

また本発明にかかるサーバ計算機保護方法によれば、

不特定のクライアント計算機によるDoS攻撃からサーバ計算機を保護するサーバ計算機保護方法であって、

クライアント計算機から送られてくるデータ要求をサーバ計算機の代わりに受け付けるステップと、

一定期間内に、すべてのクライアント計算機から届いたデータ要求の数を計測するステップと、

一定期間内に前記サーバ計算機から前記クライアント計算機へ応答した数を計測するステップと、

前記データ要求数及び応答数を用いて前記サーバ計算機の負荷状態を求めるステップと、

前記求めた負荷状態に応じて、一定期間内に受け付けた前記データ要求のうちの、該受け付けたデータ要求数に対する一定期間内に前記サーバ計算機へ転送するデータ要求の数の割合を変化させるデータ要求転送ステップと、

を有することを特徴とするサーバ計算機保護方法
が提供される。

【００１４】

加えて、本発明にかかるサーバ計算機保護プログラムとすれば、
不特定のクライアント計算機によるDoS攻撃からサーバ計算機を保護するサーバ計算機保護プログラムであって、

所定のクライアント計算機から送られてくるデータ要求をサーバ計算機の代わりに受け付けるステップと、

一定期間内に、前記所定のクライアント計算機から届いたデータ要求の数を計測するステップと、

一定期間内に前記サーバ計算機が前記所定のクライアント計算機へ応答した数を計測するステップと、

前記データ要求数及び応答数を用いて、前記所定のクライアント計算機に対するサーバ計算機の負荷状態を求めるステップと、

前記求めた負荷状態に応じて、一定期間内に受け付けた前記所定のクライアント計算機から送られてくるデータ要求のうちの、該受け付けたデータ要求数に対する一定期間内に前記サーバ計算機へ転送するデータ要求の数の割合を変化させるデータ要求転送ステップと、
を有することを特徴とするサーバ計算機保護プログラム
が提供される。

【００１５】

さらに、本発明にかかるサーバ計算機保護装置を備えたサーバ計算機が提供される。

【００１６】

【発明の実施の形態】

（第１の実施形態）

図１に本発明の第１の実施形態におけるサーバ計算機保護装置が適用されるネットワーク構成図の一例を示す。図１では、ユーザが利用するアプリケーションが稼動する計算機であるクライアント１０１－１、１０１－２、１０１－３と、

ネットワーク１０２およびサーバ保護装置１０３が存在する。また、クライアント１０１で稼動するアプリケーションの実行に伴って必要となるデータの要求を、サーバ計算機保護装置１０３を介して受信し、さらにサーバ計算機保護装置１０３を介して送信する計算機であるサーバ１０４とからなる。クライアント１０１はサーバ１０４へ処理に必要なデータを要求し、サーバ１０４はこの要求に応じてデータを応答するサーバ・クライアント型のネットワークシステムである。クライアント１０１とサーバ１０４との通信は、すべてサーバ計算機保護装置１０３を介して行われる。

【００１７】

図２に本発明の第１の実施形態におけるサーバ計算機保護装置１０３の構成図の一例を示す。サーバ計算機保護装置１０３は、データ要求受け付け部２０１、データ要求転送部２０２、データ要求計測部２０３、データ供給数計測部２０４および応答確率算出部２０５からなる。

【００１８】

クライアント１０１はサーバ計算機保護装置１０３を介してサーバ１０４との接続を確立した後、処理に必要なデータをサーバ１０４に対して要求する。このときデータ要求受け付け部２０１によって、サーバ１０４に対する要求を受け付けるとともに、データ要求数計測部２０３によって受け付け中の要求の数を計測する。

【００１９】

データ要求受け付け部２０１によって受け付けられた要求は、データ要求転送部２０２によってサーバ１０４へと転送される。サーバ１０４はこの転送された要求に対するデータを、サーバ計算機保護装置１０３を介して、この要求を行ったクライアント１０１に向けて送信する。このときサーバ計算機保護装置１０３が備えるデータ供給数計測部２０４は、サーバ１０４のこの送信によって、受け付け済みの要求の完了数を計測する。つまりクライアント１０１に対してすべての応答が完了したときには、データ要求数計測部２０３で計測した受け付け中の要求数と、データ供給数計測部２０４で計測した完了済み要求数が一致することになる。

【００２０】

仮に、データ要求数計測部２０３で計測された受け付け中の要求数が、データ供給数計測部２０４で計測した完了済み要求数よりも多い場合を考える。受け付け中の要求数が完了済み要求数より多いということはすなわち受け付けた要求に対する処理について、サーバ１０４の処理が遅れている（処理が重い）ことを意味する。完了済み要求数よりも受け付け中の要求数が増加していけば行くほどサーバ１０４の応答は遅延し、ひいてはサーバ１０４が提供しているサービスがすべて停止してしまうことも考えられる。この状態はサーバ１０４がクライアント１０１からDoS攻撃を受けた状態と同じである。サーバ１０４の管理者はサーバ１０４の停止を回避するため、クライアント１０１からサーバ１０４へ送信される要求を速やかに停止させなければならない。

【００２１】

しかしながらクライアント１０１はあくまで正当なデータ要求を行っているだけであるとすれば、この決定によってクライアント１０１で稼動するアプリケーションの処理が中断あるいは処理そのものができないことになる。

【００２２】

上記したような不具合を緩和するために、応答確率算出部２０５は受け付け中の要求数と完了済み要求数の差を元に、応答確率を少なくとも指示を行う都度算出し、これをデータ要求転送部２０２に指示する。ここでいう応答確率とは、一定期間内に受け付けたクライアント１０１からのデータ要求の数に対して、サーバ１０４が一定期間内に応答したデータ応答数の比率をいう。データ要求転送部２０２は、この値が大きければ一定期間内に受け付けたデータ要求のうち一定期間内にサーバ１０４へ転送するデータ要求の数を増やし、逆に小さければ一定期間内にサーバ１０４へ転送するデータ要求の数を減らす。

【００２３】

一定期間内に転送される要求数を減らしたために、データ要求転送部２０２によって転送されなかったデータ要求は、データ要求受け付け部２０１から破棄される。あるいは破棄することなくデータ要求受け付け部２０１に保留するようにしてもよい。ただし破棄をせずデータ要求を保留する場合には、保留したデータ

要求を、新たなデータ要求とは非同期に転送するための構成を必要とするが、本実施形態では説明しない。

【００２４】

応答確率算出部２０５は、受け付け中の要求数と完了済み要求数との差が少なくなるとサーバ１０４の負荷が軽いと判断して応答確率を高く算出し、また各要求数の差が大きくなるとサーバ１０４の負荷が高いと判断し応答確率を低く算出する。

【００２５】

上記のように構成すると、サーバに負荷をかけて停止させるようなDoS攻撃の影響を緩和させるとともに、正当なデータ要求を行っているにもかかわらずDoS攻撃をしていると判定されたクライアントの処理も停止させることのないサーバ計算機保護装置とすることができる。

【００２６】

なお、データ要求数計測部２０３の受け付け中の要求数とデータ供給数計測部２０４が計測する完了済み要求数のそれぞれの数は、たとえば前者を加算、後者を減算するようにして差分値のみを保持するようにしてもよい。結果的に両者の比較が可能な手段で蓄積されていれば足りる。

【００２７】

図３に本発明の第１の実施形態におけるサーバ計算機保護装置の動作フローの一例を示す。

【００２８】

サーバ計算機保護装置１０３を介してクライアント１０１からサーバ１０４への接続が確立された後、クライアント１０１からサーバ１０４に向けてデータ要求がされるのを待つ（Ｓ１）。データの要求がされたならばデータ要求数計測部２０３によって、応答確率算出部２０５が保持する受け付け中の要求数を１増加させる（Ｓ２）。

【００２９】

データ要求受け付け部２０１によって受け付けられたクライアント１０１からのデータ要求は、データ要求転送部２０２によってサーバ１０４へ転送しても良

いものかどうかが判断される（Ｓ３）。ステップＳ３の判断に際しては、未完了の受け付け中の要求数が使用される。

【００３０】

一定期間内のデータ応答数が一定期間内に受け付けたデータ要求数に近いほど、つまり未完了の受け付け要求数が少ないほどサーバ１０４の負荷が軽いと判断できる。逆に、一定期間内に受け付けたデータ要求数よりも一定期間内のデータ応答数が少ないほど、つまり未完了の受け付け要求数が多いほどサーバ１０４がデータ要求に対する処理を所定の時間内に完了できていない、すなわち負荷が重いと判断できる。このときの負荷が極めて重い場合には、サーバ１０４はDoS攻撃を受けている可能性が高いと判断できる。

【００３１】

上記したような理由からステップＳ３の判定に、未完了の受け付け要求数を、サーバ１０４の負荷状態として採用することができる。これはすなわち未完了の受け付け要求数が、サーバ１０４がDoS攻撃を受けていかどうかという判別にも使用できることを意味している。ステップＳ３では、この未完了の受け付け要求数に応じてクライアント１０１からの新たなデータ要求を転送しても良いかどうかを判断する。未完了の受け付け要求数がより少なければサーバ１０４に余裕があるので新たなデータ要求を転送すべきと判断し、逆により多ければDoS攻撃を受けている可能性があるので新たなデータ要求を破棄すべきと判断する。

【００３２】

このときサーバ１０４にクライアント１０１からの新たなデータ要求を転送すべきと判断したときは、このデータ要求をサーバ１０４に転送する（Ｓ４）。一方、転送しないと判断したときはこのデータ要求をデータ要求受け付け部２０１から破棄し、再びクライアント１０１からの新たなデータ要求を待つ（Ｓ１）。

【００３３】

クライアント１０１からのデータ要求をサーバ１０４に転送したときには、次にこのデータ要求に対するサーバ１０４からの応答があるので、これをクライアント１０１に対して転送する（Ｓ５）。

【００３４】

そしてこの応答からデータ供給数計測部２０４によって完了済みの要求を計測し、応答確率算出部２０５が保持する受け付け中の要求数を１減少させる（Ｓ６）。　クライアント１０１からサーバ１０４への接続が確立されたままならば再び同様の動作フローを繰り返し、クライアント１０１からサーバ１０４に向けて新たなデータ要求がされるのを待つ（Ｓ１）。

【００３５】

このようなフローによるサーバ計算機保護方法によれば、サーバに負荷をかけて停止させるようなDoS攻撃の影響を緩和させるとともに、正当なデータ要求を行っているにもかかわらずDoS攻撃をしていると判定されたクライアントの処理も停止させることのないサーバ計算機保護装置とすることができる。

【００３６】

（第２の実施形態）

図１に本発明の第２の実施形態における、サーバ計算機保護装置が適用されるネットワーク構成図の一例を示す。図１では、ユーザが利用するアプリケーションが稼動する計算機であるクライアント１０１－１、１０１－２、１０１－３と、ネットワーク１０２およびサーバ保護装置１０３が存在する。また、クライアント１０１で稼動するアプリケーションの実行に伴って必要となるデータの要求を、サーバ計算機保護装置１０３を介して受信し、さらにサーバ計算機保護装置１０３を介して送信する計算機であるサーバ１０４とからなる。クライアント１０１はサーバ１０４へ処理に必要なデータを要求し、サーバ１０４はこの要求に応じてデータを応答するサーバ・クライアント型のネットワークシステムである。クライアント１０１とサーバ１０４との通信は、すべてサーバ計算機保護装置１０３を介して行われる。

【００３７】

図４に本発明の第２の実施形態におけるサーバ計算機保護装置１０３の構成図の一例を示す。サーバ計算機保護装置１０３は、データ要求受け付け部２０１、データ要求転送部２０２、データ要求計測部２０３、データ供給数計測部２０４および応答確率算出部２０５からなる。図２に示した本発明の第１の実施形態におけるサーバ計算機保護装置１０３との相違は、データ要求数計測部２０３及び

応答確率算出部２０５を複数備えていることである。これら複数の各計測部は、複数あるクライアント１０１（たとえばクライアント１０１－１、１０１－２、１０１－３）のそれぞれから送信されるデータ要求の転送を、それぞれのクライアントごとに処理するために構成されている。クライアントごとの処理を行うためには、処理すべき要求がどのクライアントが発信したものであるかの判別が必要となる。この判別は、各クライアントから送信されるデータ要求に含まれるパケットのヘッダ情報の送信元を示すＩＰアドレスを参照することにより可能である。同様にサーバが行うサーバ応答の宛先のクライアントも、サーバ応答に含まれるパケットのヘッダ情報の宛先を示すＩＰアドレスを参照することにより判別可能である。

【００３８】

各構成要素の動作は第１の実施形態のものと同じである。

【００３９】

図５に本発明の第２の実施形態におけるサーバ計算機保護装置の動作フローの一例を示す。

【００４０】

サーバ計算機保護装置１０３を介してクライアント１０１からサーバ１０４への接続が確立され、そのクライアント１０１にデータ要求数計測部２０３と応答確率算出部２０５の組が割り当てられた後、クライアント１０１からサーバ１０４に向けてデータ要求がされるのを待つ（Ｓ１）。データの要求がされたならばそのデータ要求を行ったクライアント１０１に割り当てられているデータ要求数計測部２０３によって、その組となっている応答確率算出部２０５が保持する受け付け中の要求数を１増加させる（Ｓ７）。

【００４１】

データ要求受け付け部２０１によって受け付けられた所定のクライアント１０１からのデータ要求は、データ要求転送部２０２によってサーバ１０４へ転送しても良いものかどうかが判断される（Ｓ３）。ステップＳ３の判断に際しては、未完了の受け付け中の要求数が使用される。

【００４２】

一定期間内のデータ応答数が一定期間内に受け付けたデータ要求数に近いほど、つまり未完了の受け付け要求数が少ないほど所定のクライアント１０１によるサーバ１０４の負荷が軽いと判断できる。逆に、一定期間内に受け付けたデータ要求数よりも一定期間内のデータ応答数が少ないほど、つまり未完了の受け付け要求数が多いほどサーバ１０４が所定のクライアント１０１によるデータ要求に対する処理を所定の時間内に完了できていない、すなわち負荷が重いと判断できる。このときの負荷が極めて重い場合には、サーバ１０４はDoS攻撃を受けている可能性が高いと判断できる。

【００４３】

上記したような理由からステップＳ３の判定に、未完了の受け付け要求数を、サーバ１０４の負荷状態として採用することができる。これはすなわち未完了の受け付け要求数が、サーバ１０４がDoS攻撃を受けていかどうかという判別にも使用できることを意味している。ステップＳ３では、この未完了の受け付け要求数に応じて所定のクライアント１０１からの新たなデータ要求を転送しても良いかどうかを判断する。未完了の受け付け要求数がより少なければサーバ１０４に余裕があるので新たなデータ要求を転送すべきと判断し、逆により多ければDoS攻撃を受けている可能性があるので新たなデータ要求を破棄すべきと判断する。

【００４４】

このときサーバ１０４に所定のクライアント１０１からの新たなデータ要求を転送すべきと判断したときは、このデータ要求をサーバ１０４に転送する（Ｓ８）。一方、転送しないと判断したときはこのデータ要求をデータ要求受け付け部２０１から破棄し、再び所定のクライアント１０１からの新たなデータ要求を待つ（Ｓ１）。

【００４５】

所定のクライアント１０１からのデータ要求をサーバ１０４に転送したときには、次にこのデータ要求に対するサーバ１０４からの応答があるので、これを所定のクライアント１０１に対して転送する（Ｓ５）。

【００４６】

そしてこの応答からデータ供給数計測部２０４によって完了済みの要求を計測

し、所定のクライアント１０１に割り当てられた応答確率算出部２０５が保持する受け付け中の要求数を１減少させる（Ｓ９）。　所定のクライアント１０１からサーバ１０４への接続が確立されたままならば再び同様の動作フローを繰り返し、所定のクライアント１０１からサーバ１０４に向けて新たなデータ要求がされるのを待つ（Ｓ１）。

【００４７】

このようなフローによるサーバ計算機保護方法によれば、サーバに負荷をかけて停止させるようなDoS攻撃の影響を緩和させるとともに、正当なデータ要求を行っているにもかかわらずDoS攻撃をしていると判定されたクライアントを停止させることなく、またクライアントごとのきめ細かなサーバ計算機保護のための制御を可能としたサーバ計算機保護装置とすることができる。

【００４８】

（第２の実施形態における変形例）

本実施形態の変形例として、サーバ１０４に本実施形態にかかるサーバ計算機保護装置１０３の構成を組み合わせたサーバ１０４とすることができる。このように構成するとクライアント１０１からのデータ要求を処理するサーバ１０４と、このサーバ１０４を不特定のクライアント１０１からのDoS攻撃から保護する目的で設けるサーバ計算機保護装置１０３とを分離して個別に構成する必要がない。よってサーバ計算機保護装置１０３とサーバ１０４との通信をネットワーク等を介して行う必要がなくなり、通信に要していた時間を排除することができる。また複数の筐体により構成したサーバ計算機保護装置１０３によって保護されたサーバ１０４の場合と比較して、同様の機能を１つの筐体で提供できる可能性があり、この場合には設置に必要なスペースを削減することができる。

【００４９】

【発明の効果】

不特定のクライアントからのDoS攻撃からサーバとなる計算機を保護しながらも、正当なアクセスを行っているクライアントでありながらDoS攻撃を行っていると判断された計算機のアクセスも限定的に許容するサーバ計算機保護装置とすることができる。

【図面の簡単な説明】

【図１】　本発明の第１の実施形態にかかるサーバ計算機保護装置が適用されるネットワーク構成図の一例を示す図である。

【図２】　本発明の第１の実施形態にかかるサーバ計算機保護装置の構成図の一例を示す図である。

【図３】　本発明の第１の実施形態にかかるサーバ計算機保護装置の動作フローの一例を示す図である。

【図４】　本発明の第２の実施形態にかかるサーバ計算機保護装置の構成図の一例を示す図である。

【図５】　本発明の第２の実施形態にかかるサーバ計算機保護装置の動作フローの一例を示す図である。

【符号の説明】

１０１－１　・・・　クライアント

１０１－２　・・・　クライアント

１０１－３　・・・　クライアント

１０２　・・・　ネットワーク

１０３　・・・　サーバ計算機保護装置

１０４　・・・　サーバ

２０１　・・・　データ要求受け付け部

２０２　・・・　データ要求転送部

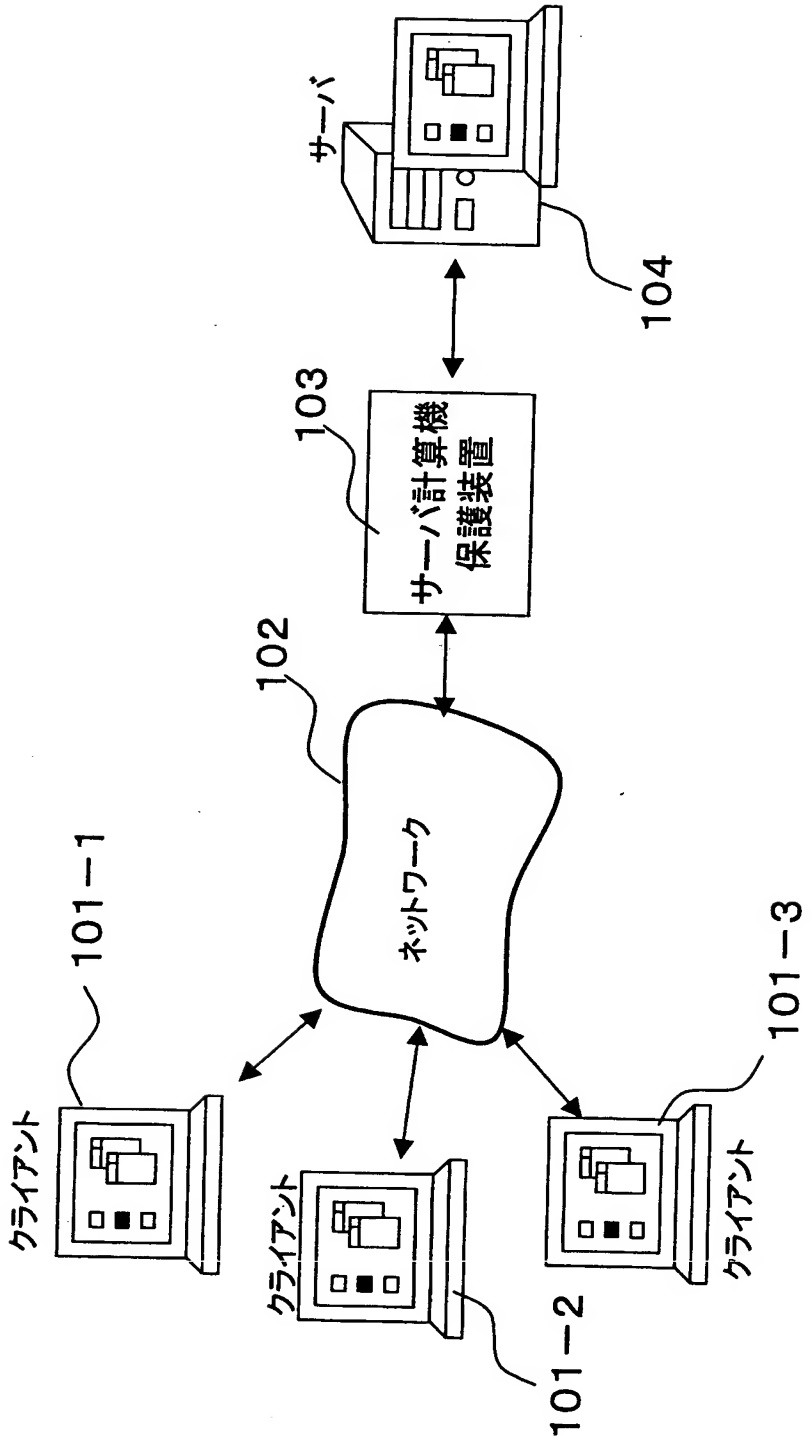
２０３　・・・　データ要求数計測部

２０４　・・・　データ供給数計測部

２０５　・・・　応答確率算出部

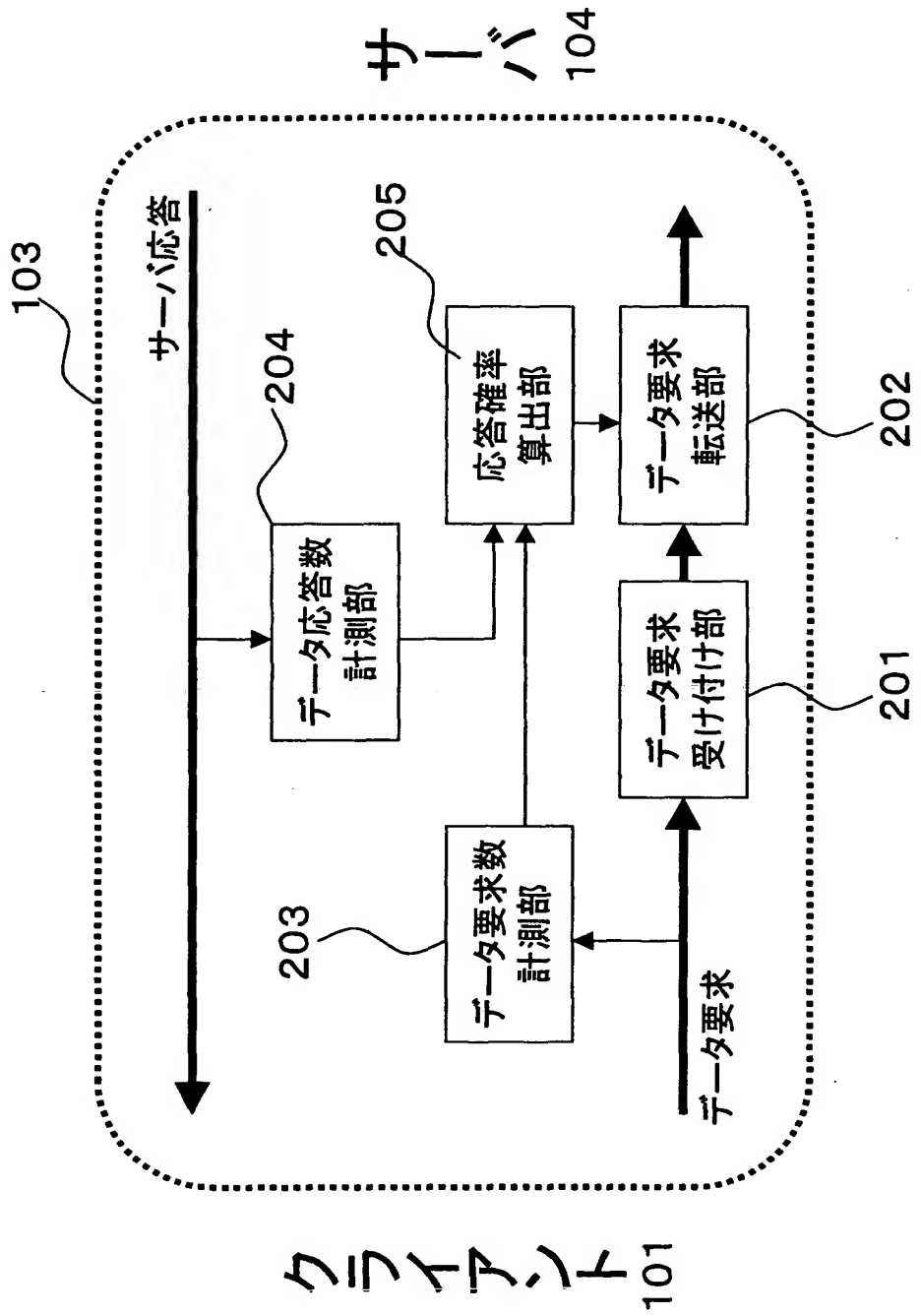
【書類名】　　図面

【図１】

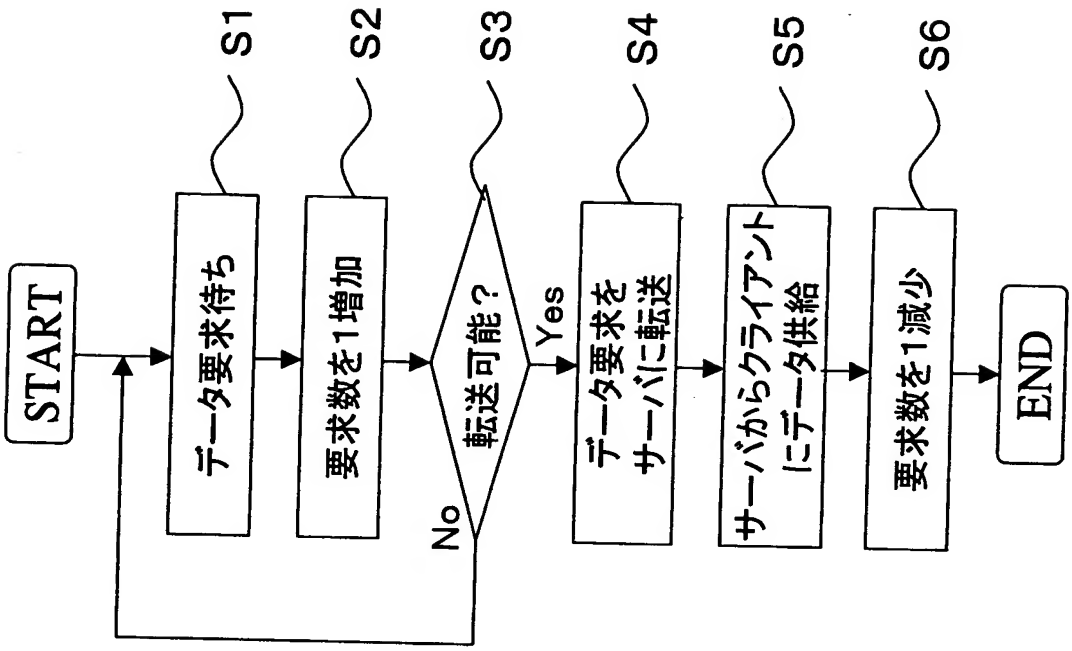


出証特２００３－３０１４０９０

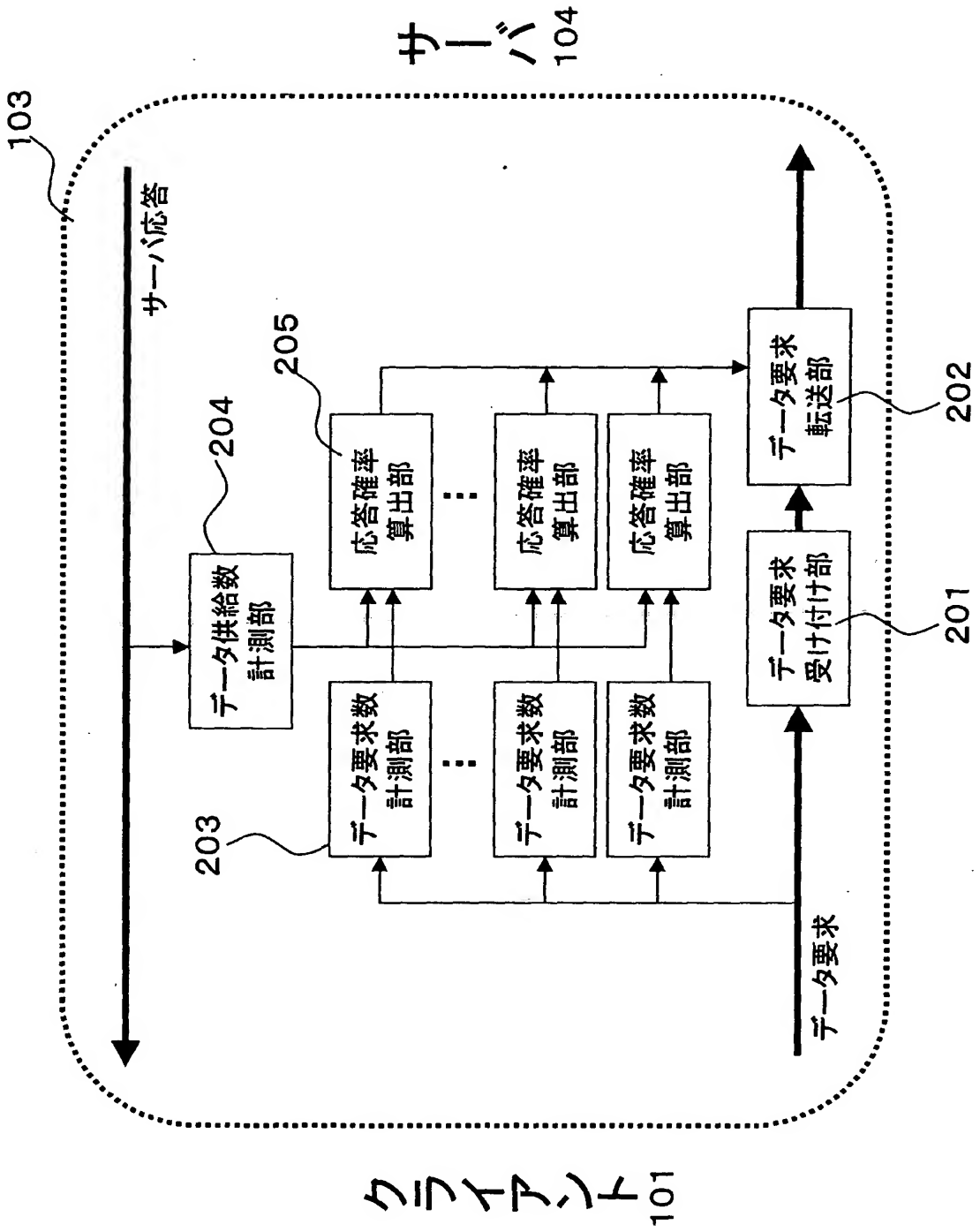
【図２】


サーバ
104
103
サーバ応答
205
204
応答確率
算出部
データ要求
転送部
202
データ応答数
計測部
データ要求
受付け部
201
203
データ要求数
計測部
データ要求
クライアント
101

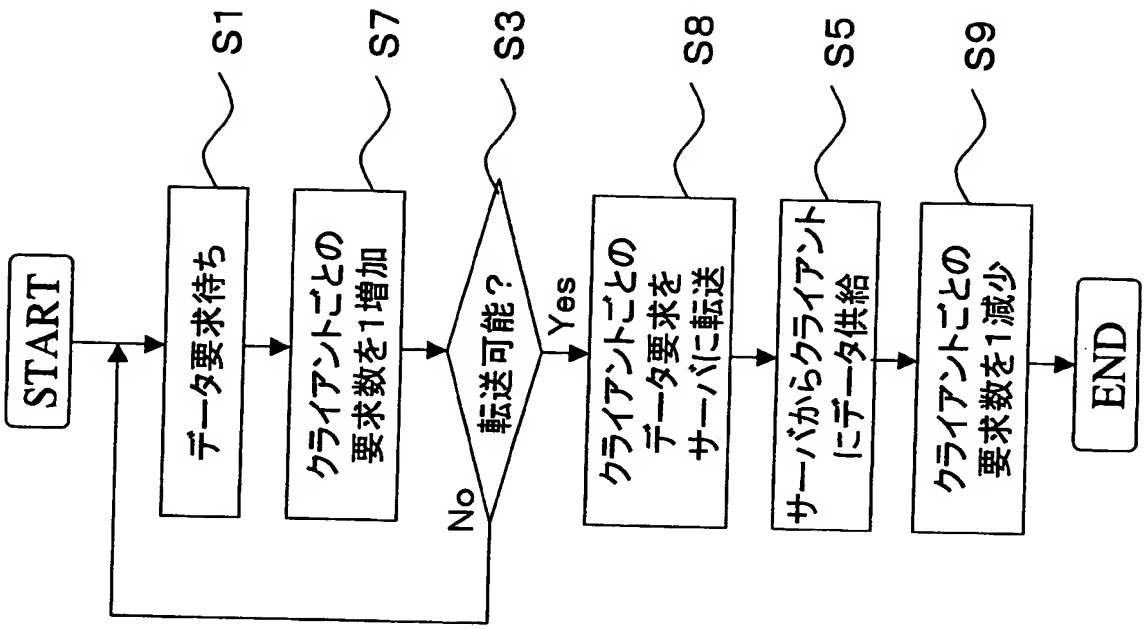
【図３】


START
データ要求待ち
S1
要求数を1増加
S2
転送可能？
S3
No
Yes
データ要求をサーバに転送
S4
サーバからクライアントにデータ供給
S5
要求数を1減少
S6
END

【図４】


サーバ
104
103
サーバ応答
205
204
データ供給数
計測部
応答確率
算出部
応答確率
算出部
応答確率
算出部
データ要求
転送部
202
データ要求
受け付け部
201
203
データ要求数
計測部
データ要求数
計測部
データ要求数
計測部
データ要求
クライアント
101

【図５】


START
データ要求待ち
S1
クライアントごとの
要求数を1増加
S7
転送可能？
S3
No
Yes
クライアントごとの
データ要求を
サーバに転送
S8
サーバからクライアント
にデータ供給
S5
クライアントごとの
要求数を1減少
S9
END

【書類名】　要約書

【要約】

【課題】　不特定のクライアントからのDoS攻撃からサーバとなる計算機を保護しながらも、正当なアクセスを行っているクライアントでありながらDoS攻撃を行っていると判断された計算機のアクセスも限定的に許容するサーバ計算機保護装置を提供することを目的とする。

【解決手段】　サーバとなる計算機に対してデータ要求される数と、これに応答するサーバのデータ応答の数を用いてサーバ計算機の負荷状態を求め、この負荷状態に応じてサーバに転送するデータ要求の割合を変化させる手段を備えたサーバ計算機保護装置とする。

【選択図】　図２

認定・付加情報

特許出願の番号	特願２００２－２８０２８９
受付番号	５０２０１４３８０７４
書類名	特許願
担当官	第八担当上席　　００９７
作成日	平成１４年　９月２７日

＜認定情報・付加情報＞

【提出日】　平成14年 9月26日

次頁無

出　願　人　履　歴　情　報

識別番号　　〔０００００３０７８〕

１．変更年月日　　２００１年　７月　２日
　［変更理由］　　住所変更
　　住　所　　東京都港区芝浦一丁目１番１号
　　氏　名　　株式会社東芝